



LES OBLIGATIONS DES ORGANISMES
COMMUNAUTAIRES SELON LA LOI 25 SUR LA
PROTECTION DES RENSEIGNEMENTS
PERSONNELS (RP)



1. Qu'est-ce que la loi 25 et qui est concerné?
2. Qu'est-ce qu'un renseignement personnel (RP)?
3. Les obligations de la loi
4. Bonnes pratiques
5. Déclaration des incidents
6. La politique de confidentialité
7. Références

Qu'est-ce que la loi 25 et qui est concerné?

Pour mieux protéger les RP détenus par les entités autres que le secteur public, déjà bien encadré.

Pour encadrer l'utilisation des RP dans un univers technologique.

S'applique à toutes les entités qui sont sous la loi III des compagnies, dont les OBNL et les organismes communautaires

Qu'est-ce qu'un renseignement personnel (RP)?

Est un renseignement personnel, tout renseignement qui concerne une personne physique et permet, directement ou indirectement, de l'identifier.

Types de RP détenus par les organismes communautaires (nom, âge, numéro de compte bancaire, notes au dossier, formulaire médical) et les utilisations possibles (prendre contact avec la personne, faire un suivi psychosocial, faire une transaction).

Les obligations de la loi

PREMIÈRE ÉCHÉANCE : 22 SEPTEMBRE 2022

Désignation du responsable de la protection des renseignements personnels (RPRP)

- Identifier au sein de votre organisation la personne compétente pour remplir ce rôle et assumer cette responsabilité;
- À défaut de désignation, c'est la personne qui a la plus haute autorité au sein de l'organisation qui sera le RPRP (directeur général, président, etc.);
- Les coordonnées du responsable de la protection des renseignements personnels doivent être publiées sur le site web de votre organisme communautaire;

Les obligations de la loi

PREMIÈRE ÉCHÉANCE : 22 SEPTEMBRE 2022

Signalement des incidents de confidentialité

- Mettre en place une procédure permettant d'identifier, de déclarer, et de gérer les incidents de confidentialité;
- Tenir un registre des incidents de confidentialité;
- Être prêt à envoyer une notification aux autorités et aux victimes;
- Disposer d'un plan d'urgence en cas d'incident de confidentialité

DEUXIÈME ÉCHÉANCE : 22 SEPTEMBRE 2023

Politique de confidentialité :

- Mettre en place une politique de confidentialité;
- Publication sur le site Web de votre organisme communautaire;

Politiques et pratiques encadrant la gouvernance à l'égard des renseignements personnels :

- Mettre en place ces politiques et pratiques;
- Publier une information détaillée au sujet de ces politiques et pratiques sur le site web de votre organisme communautaire;

Les obligations de la loi

DEUXIÈME ÉCHÉANCE : 22 SEPTEMBRE 2023

Consentement et transparence

- Obtenir des usagers / bénéficiaires un consentement manifeste, libre et éclairé à des fins spécifiques;
- Fournir les informations prévues par la loi au moment de la collecte des renseignements personnels (transparence);

Conservation et destruction

- Mettre en place une politique de conservation et de destruction des renseignements personnels conformément aux finalités de la collecte et / ou aux délais prévus par la loi ou les règlements.

Les obligations de la loi

TROISIÈME ÉCHÉANCE : 22 SEPTEMBRE 2024

Droit à la portabilité

Votre organisme communautaire devra être capable de communiquer à la personne concernée ses renseignements personnels informatisés dans un format technologique structuré et couramment utilisé ou de répondre à une demande de transfert de ses renseignements personnels à tout organisme/personne autorisée par la loi.

Les obligations de la loi

Bonnes pratiques

- Faire l'inventaire des RP détenus et tenir à jour cet inventaire;
- Préciser les rôles et responsabilités des employéEs impliquéEs dans la protection des RP;
- Rédiger et faire remplir systématiquement le consentement des personnes collectées;
- Le faire signer sur un papier distinct;
- Traiter les demandes et les plaintes des participantsEs concernant les RP;
- Rendre un RP facile à obtenir en consultant votre système informatique dans le but de le communiquer à une personne autorisée par la Loi ou son statut à le recueillir.

Déclaration des incidents

Un incident de confidentialité peut être un événement de cybersécurité ou provenant d'une erreur humaine.

Un avis d'incident doit alors être rempli et doit comprendre les renseignements suivants :

- Les circonstances de l'atteinte;
- La date ou la période où il y a eu atteinte;
- La nature des renseignements personnels visés par l'atteinte;
- Les mesures que l'organisation a prises afin de réduire le risque de préjudice qui pourrait résulter de l'atteinte;
- Les mesures que peut prendre tout intéressé afin de réduire le risque de préjudice qui pourrait résulter de l'atteinte;
- Les coordonnées permettant à l'intéressé de se renseigner davantage sur l'atteinte.

La politique de confidentialité

La politique devrait contenir les informations suivantes:

- Le nom de la personne responsable;
- Les RP que vous recueillez et traitez;
- L'endroit où sont conservés les RP;
- Comment vous utilisez le RP que vous collectez;
- Comment vous détruisez les RP que vous avez;
- La feuille de consentement à faire remplir à toute personne dont vous récoltez des données personnelles;
- Le mécanisme de fonctionnement en ce qui concerne le traitement des plaintes;
- Le mécanisme de fonctionnement en ce qui concerne les déclarations d'incidents.

Références

[Formulaires et lettres types](#)

[Questions fréquentes Commission d'accès à l'information du Québec](#)

[Listes des organismes assujettis](#)

[Guide de conformité pour la réforme de la Loi sur la protection des renseignements personnels dans le secteur privé](#)

[L'infonuagique](#)

[Trousse d'information gratuite, Mes procédures](#)

[Exemple de politique](#)

Questions?

Anick Lorrain, directrice de la Corporation de développement communautaire de Mirabel (CDC)

Courriel: direction@cdcdemirabel.com

Téléphone: 450 848-6059

